PAF-FPE: Privacy aware content filtering for future pervasive environments

Executive Summary

Author:
Leonardo Maccari

DISI: Department of Information Engineering and Computer Science, University of Trento

March 2011 - February 2014

A Marie-Curie project financed by EU and The Trentino programme of research, training and mobility of post-doctoral researchers, incoming Post-docs 2010, grant #40101857

1 The project

The original project proposal for PAF-FPE states: *"The focus of the proposed project is the realization of a dynamic, efficient content analysis and filtering platform for wireless distributed and pervasive networks. The platform should be able to scale on the number of the wireless nodes and on the available hardware in order to be applicable to scenarios that go from wireless pervasive networks made of hundreds of nodes with limited resources, to mobile wireless mesh networks used for emergency management or connectivity distribution".*

During the development of the project the focus has been concentrated on two specific fields of application among the possible ones included in the generic term "*Pervasive networks*", that is, wireless ad-hoc (social) networks and wireless community networks (WCNs).

Social networks (SN) have developed very quickly involving millions of users that are willing to share their data to interact with each other, with a recent switch on mobile applications. Lately, There is a growing interest in moving from a purely server-based platform that uses broadband connections to a multi-hop peer-to-peer networking model that uses wireless interfaces present in most of the modern mobile devices (as a very recent example, consider the very large attention gained by the FireChat application, that implements such a model). Under a privacy point of view, ad-hoc social networks present different features compared to mainstream online social networks. First, in such a network all the communications are ephemeral, there is no centralized platform where the communication is stored permanently. Second, the communication does not require valuable resources to be possible. On-line SNs require expensive infrastructures and a business model that nowadays is mostly based on targeted advertising. If the platform is inexpensive, instead, there is no need to have a business model to support it, and the users can freely shape their interactions without a constant conflict with a third party that wants to achieve an economic benefit.

The second field of research of the project is the study of Wireless Community Networks (WCN). A WCN is a wireless mesh network created and managed by a local community of people in a certain area (a city, a town or a rural area). WCNs today are blooming in all the world, from small communities to large ones. WCNs were born to bring Internet connectivity to areas not covered by any ISP, but today they are run by lively communities of people sharing mainly internal services and community-owned applications. The most astonishing examples are represented by the AWMN and

Guifi networks[1] that account for about 2.500 and 25.000 wireless nodes respectively. WCNs present very similar challenges to ad-hoc social networks: they use distributed protocols, they are cooperatively managed (they do not have a single owner), they offer similar social applications (chat, file-sharing, games etc). The scientific interest in WCNs is currently very strong (there are at least 3 European project focused on WCNs[2]) motivated by the fact that these networks are technically challenging and socially relevant. In the light of recent privacy scandals (i.e. the Datagate scandal) the importance of community-managed, privacy-aware platforms has strongly increased.

Both these kinds of networks share similar privacy challenges. When a user participates to a wireless distributed network, where different social services are offered he will be sharing information with other network nodes in the same area, however, not all information is to be shared with everyone, and some form of protection from attacks and malicious traffic is needed. His presence is an information he might want to share only with a subset of the participants in the network. If he is sending a message to the network he might want to limit the range (in terms of wireless hops) that his messages will be forwarded to, he might want to limit the recipients to only a selected subset of users. If there is another user generating malicious traffic, some sort of collaborative protection against this event is needed.

One approach to tackle this family of challenges is to enforce a decentralize filtering/monitoring infrastructure that will leverage on the collaborative nature of such networks, and is the approach chosen in PAF-FPE.

During the project, the research has been focused on finding a way to efficiently distribute filtering (or matching rules, in general) to analyse, shape, limit the traffic in a multi-hop network, with an user-based approach. This approach has been defined the *Waterwall*, in order to express a fluid and distributed approach, opposed to the centralized approach that firewalls currently have. The waterwall relies on the distribution of user-generate rules and the enforcement of the rules on a subset of nodes, carefully chosen to minimize the impact on network performance and maximise the enforcement of the rule-sets. The proposed solution has been analysed using computer simulations and verifying its applicability through the analysis of real network topologies of large-scale wireless community networks. WCNs offer available data-sets describing topologies, traffic, signalling, protocols. These data-sets

[1] see www.awmn.net and www.guifi.org

[2] see www.confine-project.eu, www.clommunity-project.eu, www.p2pvalue.eu)

have been studied to verify if the topological properties that motivated the results on simulated topologies can be found also in the real topologies. This activity is still in progress (after the end of PAF-FPE) and its results are only partly available, being currently under review (at the time of writing this report).

The research on the waterwall is deeply connected with other network features, such as its applicability on existent routing protocols, and the security procedures and mechanisms that are needed to access and share data in a distributed wireless network. Some of these themes have been analysed during PAF-FPE and produced related publications.

2 Results

2.1 Publications

2.1.1 Congresses Proceeding papers (peer-reviewed)

- R. Lo Cigno L. Maccari. "*Urban Wireless Community Networks: Challenges and Solutions for Smart City Communications*". Invited paper to the ACM Workshop on Wireless and Mobile Technologies for Smart Cities (WiMobCity 2014).

- L. Baldesi, L. Maccari, R. Lo Cigno. "*Live P2P Streaming in CommunityLab: Experience and Insights*". To appear in Proceedings of the 13th IEEE IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2014)

- L. Maccari. "*An Analysis of the Ninux Wireless Community Network*". In the Second International Workshop on Community Networks and Bottom-up-Broadband (CNBuB) co-located with the WiMob conference, 2013

- L. Maccari and M. Rosi. "*Re-breaking Wireless Protected Setup*". Poster to the IEEE Conference on Computer Communications (Infocom), 2013.

- L. Maccari. "*A Collaborative Firewall for Wireless Ad-hoc Social Networks*". In Proceedings of the International Conference on Security and Cryptography, 2012

- L. Maccari and R. Lo Cigno. "*How to Reduce and Stabilize MPR Sets in OLSR Networks*". In The 8th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2012

- L. Maccari, R. Lo Cigno, "*Privacy in the Pervasive Era: A Distributed Firewall Approach*". In proceedings of the Annual Conference on Wireless On-demand Network Systems and Services (WONS 2012)

2.1.2 Presentations to International conferences

- L. Maccari. "*On privacy implications of distributed wireless social networks*". In Amsterdam Privacy Conference, 2012

2.1.3 International Journal papers (ISI-indexed)

- L. Maccari, R. Fantacci, T. Pecorella, G. Ghettini, and F. Chiti. "*Protecting Mobile Agents Communications in Pervasive Networks with a Trusted Distributed Mediator for ID-based RSA*". Accepted for publication in Wiley Security and Communication Networks, 2014

- L. Maccari and R. Lo Cigno. "*Waterwall: a Cooperative, Distributed Firewall for Wireless Mesh Networks*". SpringerOpen/EURASIP Journal on Wireless Communications and Networking, 2013:225 . SI on Advances in Trust, Security and Privacy for Wireless Networks.

- L. Maccari and R. Lo Cigno. "*Betweenness Estimation in OLSR-based Multi-Hop Networks for Distributed Filtering*". Elsevier Journal of Computer and System Sciences. Special issue on Wireless Networks Intrusion: 80 (3), May 2014

2.1.4 Technical Reports

- L. Maccari, R. Lo Cigno: "*Privacy in the Pervasive Era: A Distributed Firewall Approach*". Online: http://disi.unitn.it/locigno/preprints/TR-DISI-11-481.pdf

- L. Baldesi, L. Maccari, R. Lo Cigno: "*PartyHub - A Peerstreamer Conference Application*". Online: http://eprints.biblio.unitn.it/4242/1/techRep037.pdf

2.1.5 Public presentations (not peer-reviewd)

- Leonardo Maccari, Renato Lo Cigno "*Wireless Mesh Networks filtering, from a Firewall to a Waterwall*" Italian Networking Workshop, 2012
- L. Maccari "*Voglio tutto distribuito!*" Presentation to the 11th E-Privacy conference, Milan 2012
- L. Maccari "*PAF-FPE: Privacy Aware Content Filtering for Future Pervasive Environments*" presentation to the review meeting of Progetto Trentino, December 2012
- L. Maccari "*PAF-FPE: Privacy Aware Content Filtering for Future Pervasive Environments*" presentation to the review meeting of Progetto Trentino, March 2013
- L. Maccari "*An Analysis of the Ninux Wireless Community Network*". Presentation of the CNBUB results given to the Italian Ninux community in Rome, November 2013. Repeated to the CONFINE meeting, November 2013.
- L. Maccari "*Wireless Community Networks, Social, Privacy-aware Networks of People*" (Draft titile). To be held in the seminar "*Wireless Community Networks: Alcune Riflessioni in Chiave Tecnica, Sociologica e Giuridica*", Trento, Maggio 2014.
- L. Maccari "*Are Wireless Community Networks really decentralized networks?*". Presentation to the Battle of The Mesh, May 2014.

2.1.6 Submitted works

Currently, there are 4 journal papers under review in ISI-indexed journals, among which:

- L. Maccari, R. Lo Cigno. "*A Week in the Life of Three Large Wireless Community Networks*". Accepted with minor revision (currently under review) in Elsevier Ad Hoc Networks Journal, SI on "Modeling and Performance Evaluation of Wireless Ad-Hoc Networks"

2.2 Active cooperations

This section presents a brief list of the past and active cooperation at the time of writing.

- Cooperation with the OSPS, CONFINE and CLOMMUNITY project. CONFINE and CLOMMUNITY are two FIRE projects focused on research in the context of Wireless Community Networks. There is an undergoing work with the Universitat Politècnica de Catalunya (BarcelonaTech), that spans on multiple topics, from topology analysis to the use of collected data for simulator design. Leonardo Maccari will spend a month between May and June 2014 to cooperate on this topic.

- With the University of Sevilla, a scientific paper Is currently under review for the Computers & Security journal. Its focus is the new Linux firewall infrastructure, that will be of great help for the development of the concepts introduced in PAF-FPE. During the project Leonardo Maccari has spent two weeks in Sevilla cooperating with the Computer Science department.

- After the end of the PAF-FPE project, Leonardo Maccari's post-doc has been financed by the project "*Wireless Communities: legal and social implications*" funded by the CARITRO foundation together with the department of Law of the University of Trento and the department of Sociology of the University of Padua. This project can be considered a multi-disciplinary one-year follow-up of the WCN-related results of PAF-FPE and shows that the results of PAF-FPE are of high interest.

- A cooperation with a Firenze-based company, Phoops s.r.l., has produced the publication on the security of a recent wireless authentication standard (WPS). Phoops is a SME with special interest in innovation and security, and their expertise has been a key component in the that joint publication.

- A cooperation with the DINFO of the University of Florence has lead to the a publication on authentication mechanisms for distributed networks that can be used on the distributed filtering infrastructure.

- A publication currently under review has been realized together with Mirko Maishberger from Nokia (Berlin), given his expertise in the field of optimization.

2.3 Realization of new tools

During PAF-FPE, several open source projects have been realized to support the realization of publications. Among these are software simulators components to simulate ad-hoc networks, such as:

- http://pervacy.eu/musolesi-mobility-model-for-omnet
- http://pervacy.eu/chat-application-for-omnet
- http://pervacy.eu/addressgenerator-for-inet
- Software components to analyse network topolgies: http://pervacy.eu/content/new-code-and-paper-community-network-analysis

All the source code has been released with an open source license and can be downloaded and re-used by other researchers to reproduce and improve the results.

Data-sets of real topologies for WCNs have been also produced. The data are the elaboration of original data-sets needed to perform a centrality analysis, at the base of the distributed firewall proposal. Since the corresponding publications are still review pending, they are not yet fully public available, a preview is available from the url http://pervacy.eu/content/preview-community-network-monitor-data.